PDF Stamper User Manual
ELPROMA

Introduction

The main function of PDF Stamper is to sign PDF documents using X.509 digital certificates. Using this product, you can quickly sign multiple PDF files (bulk sign) by selecting input and output directory. This is ideal for bulk signing of a large number of corporate documents rather than signing each one individually. All documents will be also automatically RFC3161 time stamped to TSA.

The positioning of the signature appearance is configurable, plus on which pages of the document it should appear (first page, last page or all pages).

Links

PDF Stamper main page is: http://www.clepsydratime.com download section.

Warning and Disclaimer

Every effort has been made to make this manual as complete and accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this manual.

Trademarks

Clepsydra Time, Clepsydra Time Systems are trademarks of Elproma Elektronika Sp. o.o.
.NET, Visual Studio .NET are trademarks of Microsoft Inc.
Adobe, Adobe Reader are trademarks of Adobe Systems Inc.
All other trademarks are the property of their respective owners.

Table of context

Digital Certificates

Digital Certificate Location

To digitally sign a PDF file a digital certificate is needed. The digital certificates are stored in two places:

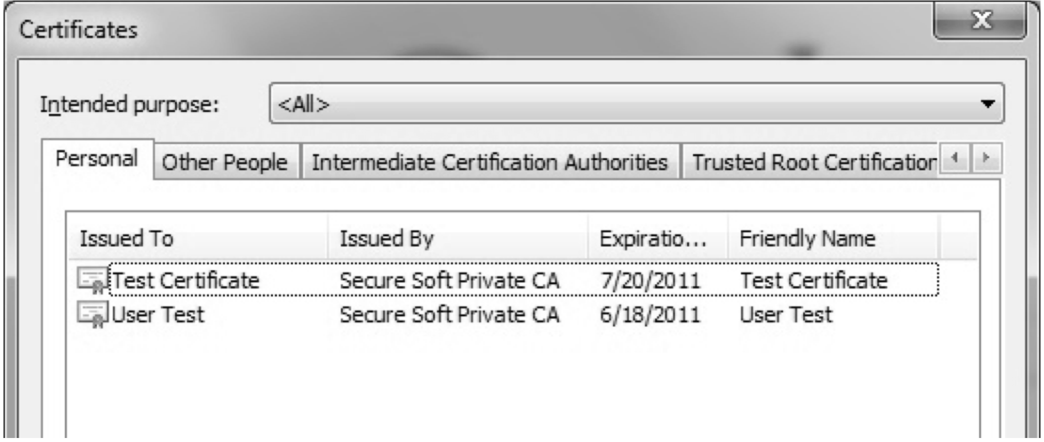
- in Microsoft Store
- in PFX on P12 files

The certificates stored on **Microsoft Store** are available by opening *Internet Explorer – Tools* menu – *Internet Options – Content* tab – *Certificates* button (see below).

For PDF digital signatures, the certificates stored on *Personal* tab are used. These certificates have a public and a private key.

The digital signature is created by using the private key of the certificate. The private key can be stored on the file system (imported PFX files), on an cryptographic smart card (like Aladdin eToken or SafeNet iKey) or on a HSM (Hardware Security Module).

Signing certificates available on Microsoft Store


Certificates
X
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Test Certificate	Secure Soft Private CA	7/20/2011	Test Certificate
User Test	Secure Soft Private CA	6/18/2011	User Test

Another way to store a digital certificate is a **PFX (or P12) file**. This file contains the public and the private key of the certificate. This file is protected by a password in order to keep safe the key pair.

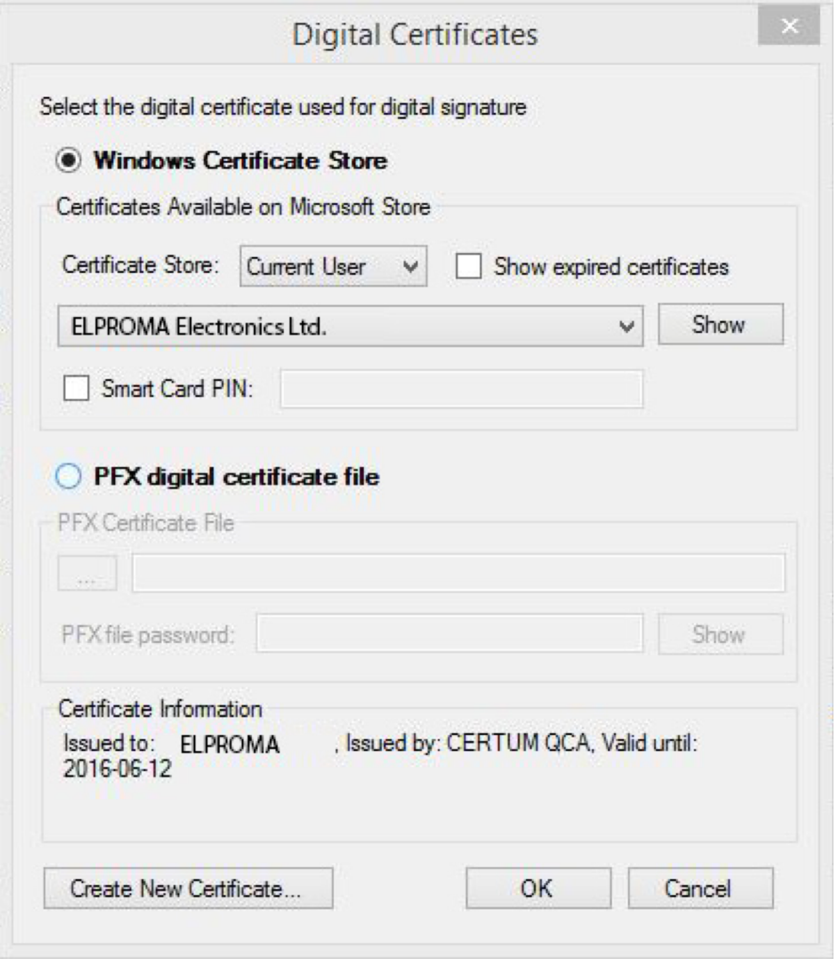
Note that a PFX file can be imported on Microsoft Store (just open the PFX file and follow the wizard). To obtain a digital certificate go to top menu and select:

Tools->Create a Digital Certificate.

Select the Digital Certificate for Creating PDF Signatures

To digitally sign a PDF, a digital certificate must be selected from Digital Certificates section. The digital certificate used to create the digital signature can be stored on Microsoft Store or a PFX file.

Select the digital certificate



Digital Certificates

Select the digital certificate used for digital signature

● **Windows Certificate Store**

Certificates Available on Microsoft Store

Certificate Store: Current User ☐ Show expired certificates

ELPROMA Electronics Ltd.

☐ Smart Card PIN:

○ **PFX digital certificate file**

PFX Certificate File

PFX file password:

Certificate Information

Issued to: ELPROMA , Issued by: CERTUM QCA, Valid until: 2016-06-12

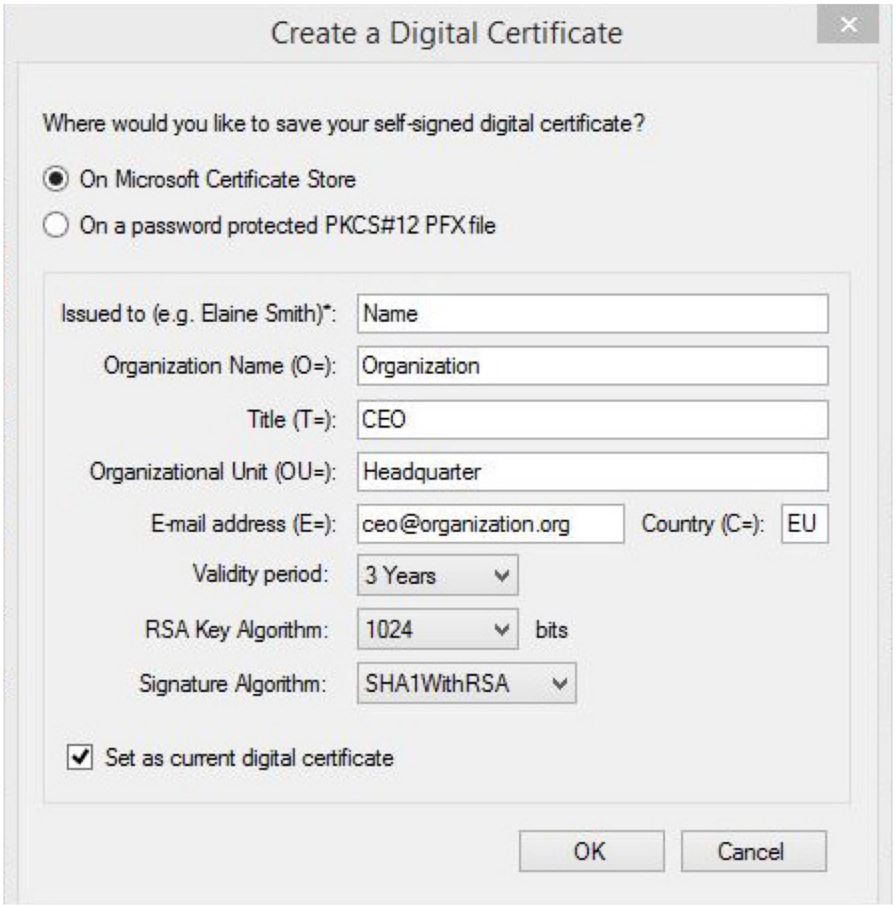
You can also create new certificate at this step by clicking button “*Create New Certificate*”.

Create a Digital Certificate

If no certificates are available on the computer, a new certificate can be created from *Create a Digital Certificate* section.

This certificate can be set as the default digital certificate used for PDF signatures.

Create a digital certificate



Where would you like to save your self-signed digital certificate?

● On Microsoft Certificate Store

○ On a password protected PKCS#12 PFX file

Issued to (e.g. Elaine Smith)*:	Name
Organization Name (O=):	Organization
Title (T=):	CEO
Organizational Unit (OU=):	Headquarter
E-mail address (E=):	ceo@organization.org
Country (C=):	EU
Validity period:	3 Years
RSA Key Algorithm:	1024 bits
Signature Algorithm:	SHA1WithRSA

☑ Set as current digital certificate

Validating Digital Signatures in Adobe

Every digital certificate is issued by a Root CA (Certification Authority). Some of the Root CA's are included by default in Windows Certificate Store (Trusted Root Certification Authorities) and only a few are included in Adobe Certificate Store. Microsoft and Adobe use different Certificate Stores different certificate validation procedures.

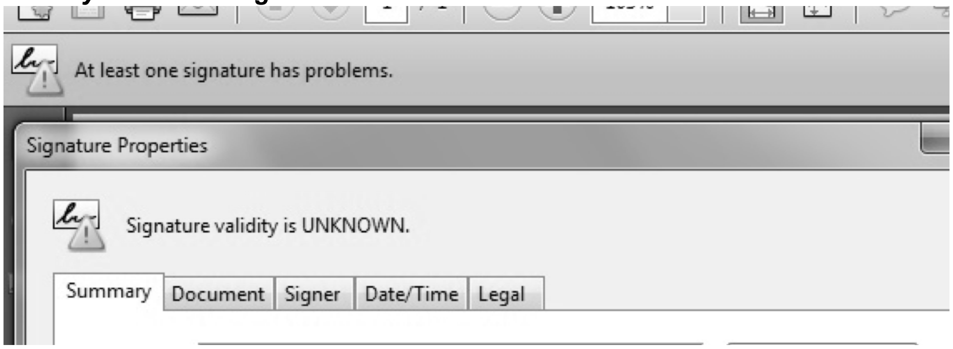
If the signing certificate (or the Root CA that issued the signing certificate) is not included in Adobe Store, the digital signature is considered "not trusted" when a user open a document with Adobe Reader (see example).

This behavior has nothing to do with the signing engine but with the Adobe certification validation procedure.

To trust a signature the user must add the signing certificate on the Adobe Certificate Store because only a few Root CA's are considered trusted by default by Adobe certificate validation engine (See this article: http://www.adobe.com/security/partners_cds.html)

To validate the signing certificate in Adobe use the methods described on this document: http://www.clepsydratime.com/file_upl/PDF/ValidatingDigitalSignaturesInAdobe.pdf

Validity Unknown signature

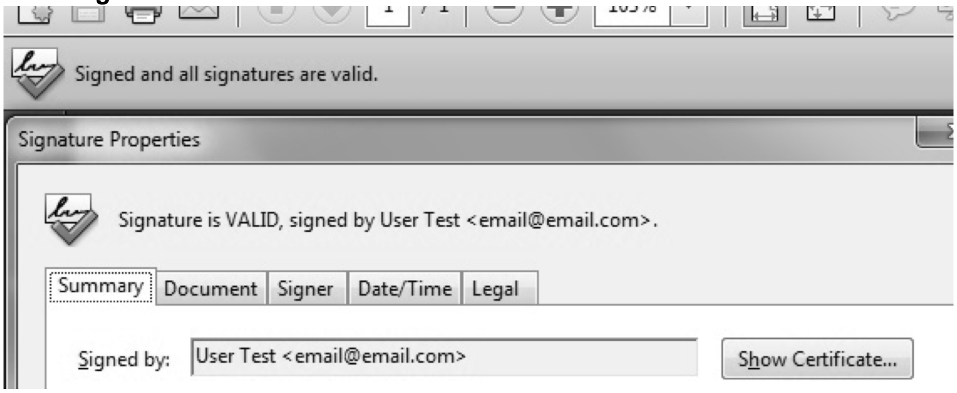


At least one signature has problems.

Signature Properties

Signature validity is UNKNOWN.

Valid signature



Signed and all signatures are valid.

Signature Properties

Signature is VALID, signed by User Test <email@email.com>.

Signed by: User Test <email@email.com>

Digital Signature Options

Digital Signature Rectangle

If the checkbox *Visible signature box* is checked, a signature rectangle will be inserted on the PDF document. The appearance of the digital signature can be customized from the *Signature Appearance* section.

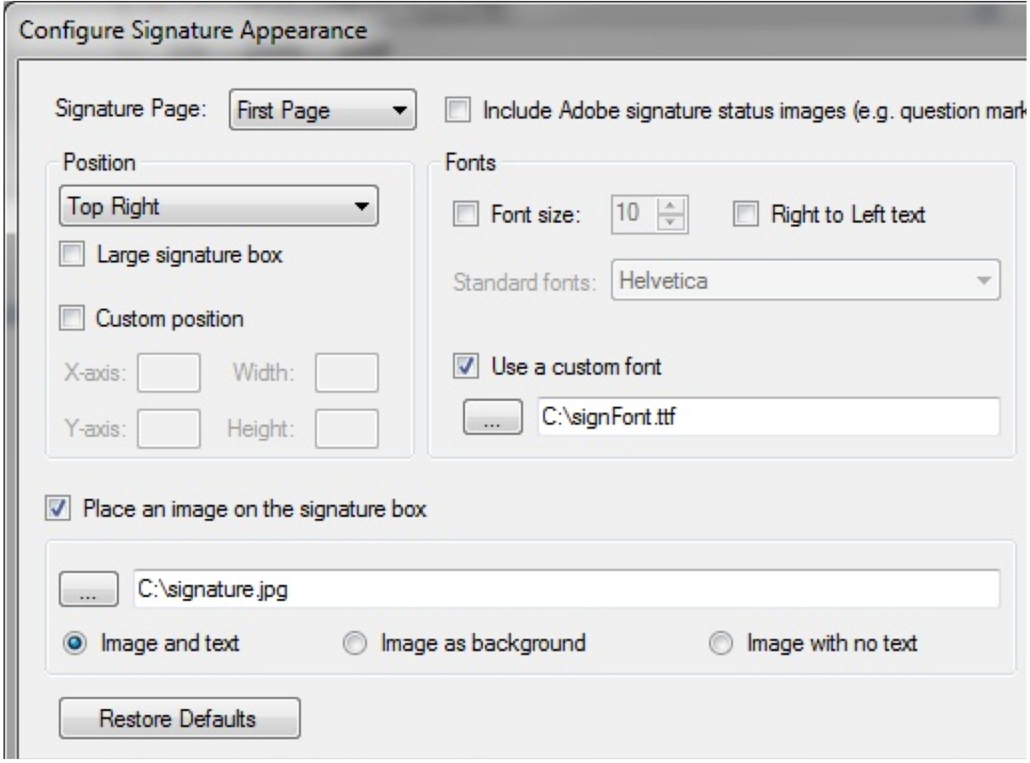
The default text direction is left to right. To change the text direction to right to left (e.g. for Hebrew language) checkbox *Right to Left text* must be checked.

The default font file for the digital signature rectangle is Helvetica. It is possible that this font to not include all necessary UNICODE characters like **ä, à, â, ą,** etc. On this case you will need to use an external font.

The font size is calculated based on the signature rectangle size in order to fit on the signature rectangle (it not have a fixed size). If you want to use a specific font size, it can be specified on the *Font size* section.

Observation: If the custom position will be used, the corner (0,0) is on the bottom left of the page.

Basic appearance settings



Configure Signature Appearance

Signature Page: First Page

□ Include Adobe signature status images (e.g. question mar

Position

Top Right

□ Large signature box

□ Custom position

X-axis: Width:

Y-axis: Height:

Fonts

□ Font size: 10

□ Right to Left text

Standard fonts: Helvetica

☑ Use a custom font

... C:\signFont.ttf

☑ Place an image on the signature box

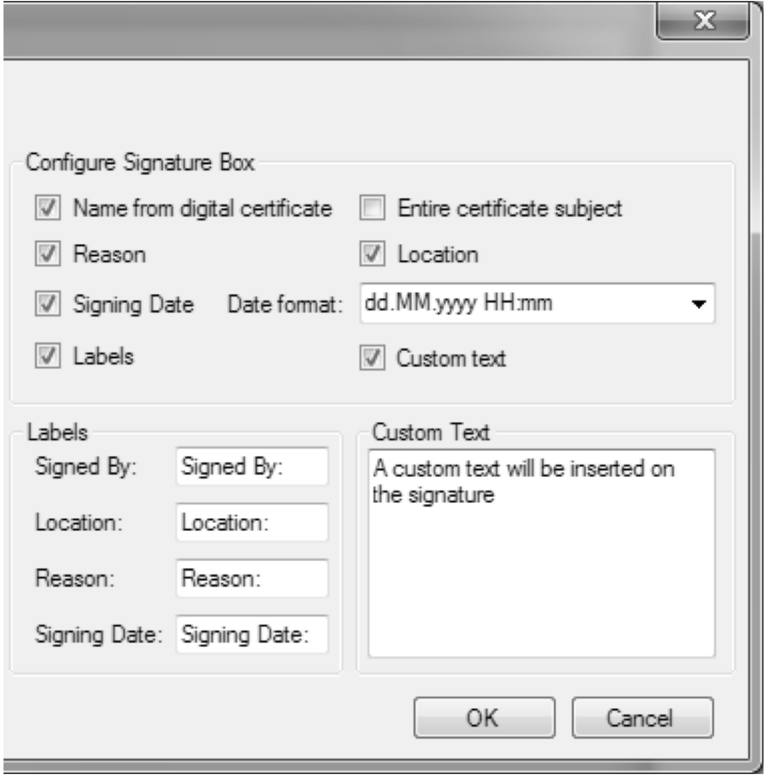
... C:\signature.jpg

● Image and text ○ Image as background ○ Image with no text

Restore Defaults

The default digital signature text contains information extracted from the signing certificate, signing date, signing reason and signing location but the digital signature text can be easily customized.

Signature text



Configure Signature Box

☑ Name from digital certificate ☐ Entire certificate subject

☑ Reason ☑ Location

☑ Signing Date Date format: dd.MM.yyyy HH:mm

☑ Labels ☑ Custom text

Labels

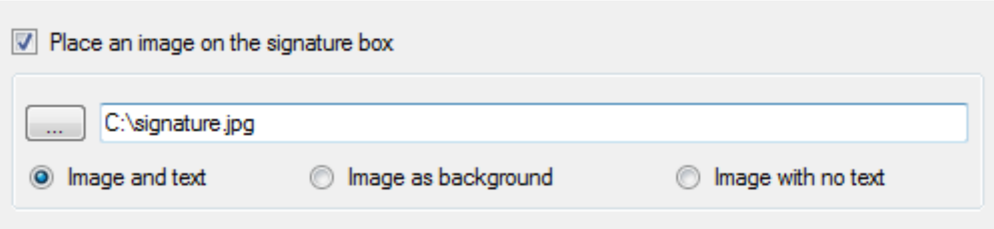
Signed By:	Signed By:
Location:	Location:
Reason:	Reason:
Signing Date:	Signing Date:

Custom Text

A custom text will be inserted on the signature

Set the Digital Signature Graphic

The digital signature rectangle can contains text, graphic or text with graphic. To add an image on the digital signature rectangle, you can do that from *Place an image on the signature box* section.



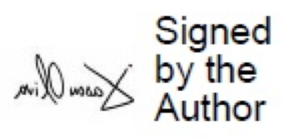
☑ Place an image on the signature box

C:\signature.jpg

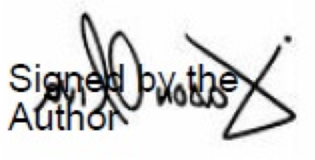
● Image and text ○ Image as background ○ Image with no text

These types of signatures are shown below:

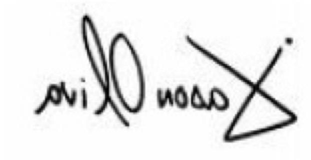
1. Image and text,



2. Image as background,

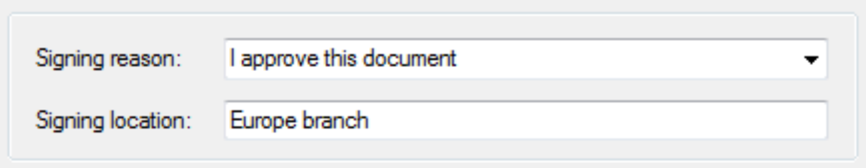


3. Image with no text



Signing Reason and Location

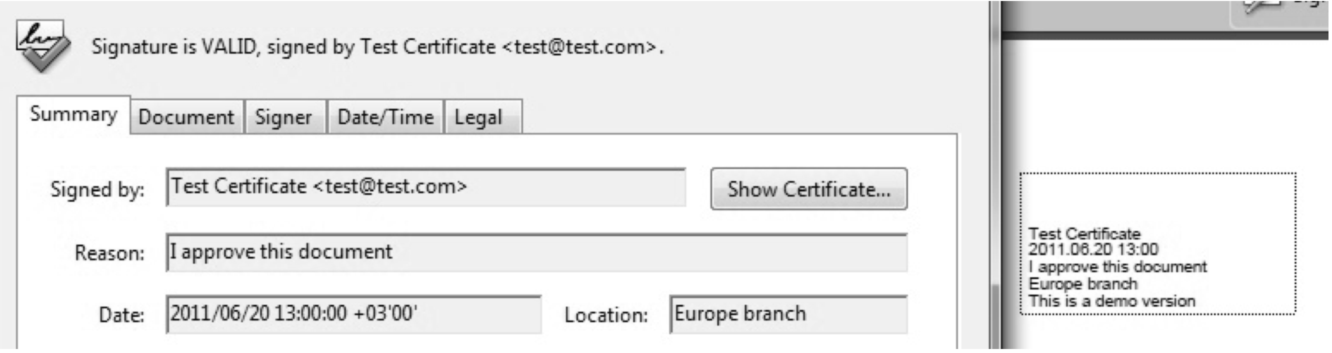
The signing reason and location attributes can be set from the main interface.



Signing reason: I approve this document

Signing location: Europe branch

Signed by, Reason, Location and Date properties in Adobe



Signature is VALID, signed by Test Certificate <test@test.com>.

Signed by: Test Certificate <test@test.com>

Reason: I approve this document

Date: 2011/06/20 13:00:00 +03'00'

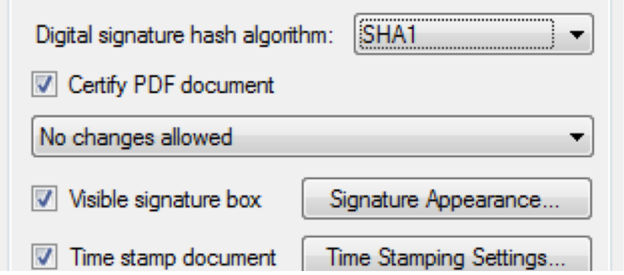
Location: Europe branch

Test Certificate
2011.06.20 13:00
I approve this document
Europe branch
This is a demo version

Using SHA256, SHA512 Hash Algorithms

The default (and recommended) hash algorithm used by the library is **SHA1** but in some cases, SHA256/384/512 must be used for the digital signature and the Time Stamp Request.

Set the Hash Algorithm



Digital signature hash algorithm: SHA1

☑ Certify PDF document

No changes allowed

☑ Visible signature box

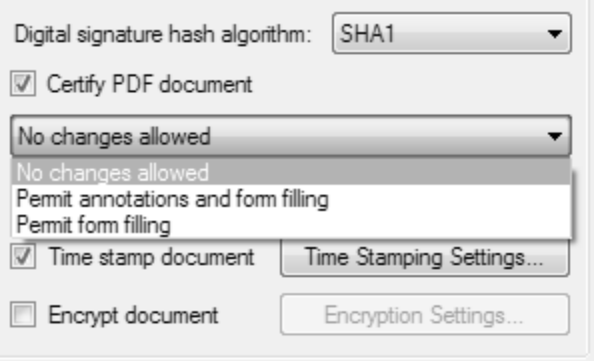
☑ Time stamp document

Certify a PDF Digital Signature

When you certify a PDF, you indicate that you approve of its contents. You also specify the types of changes that are permitted for the document to remain certified.

You can apply a certifying signature only if the PDF doesn’t already contain any other signatures. Certifying signatures can be visible or invisible. A blue ribbon icon in the Signatures panel indicates a valid certifying signature.

To certify a digital signature, select the certification type from the main interface.



Digital signature hash algorithm: SHA1

☑ Certify PDF document

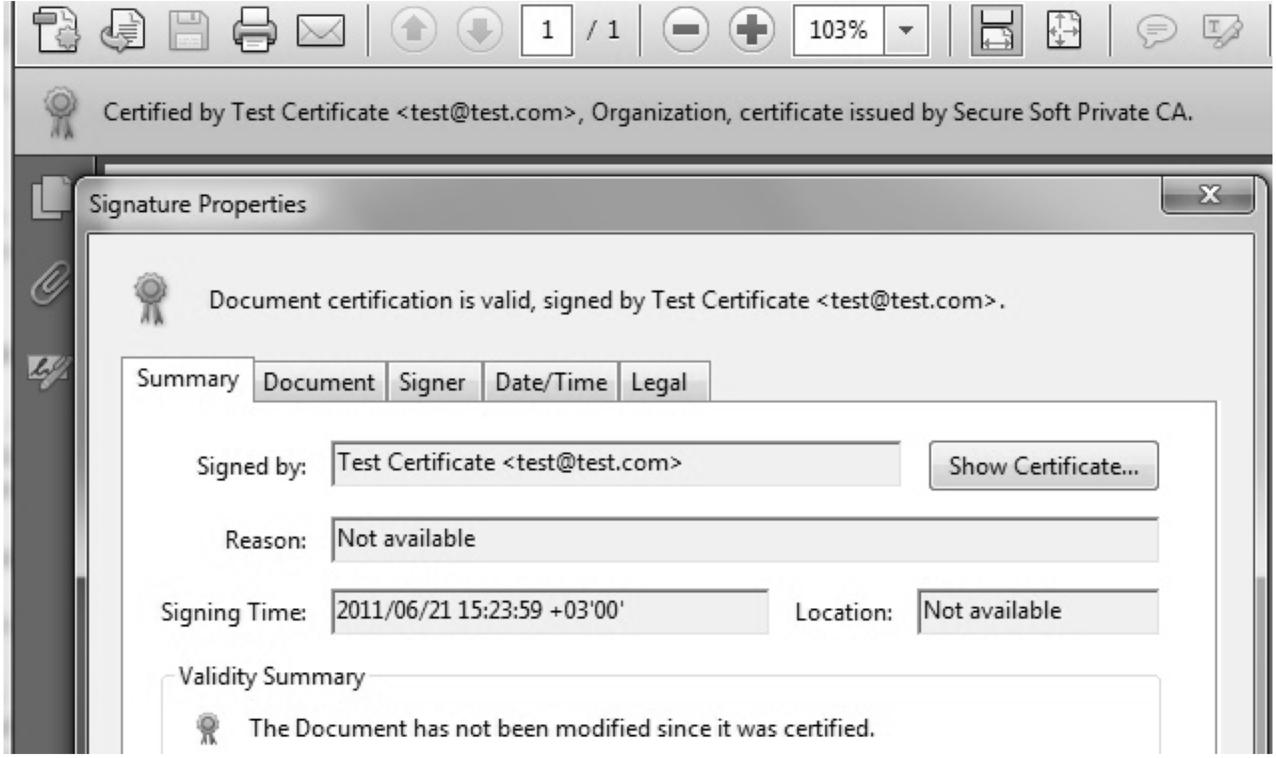
No changes allowed

☑ Time stamp document

□ Encrypt document

No changes allowed
Permit annotations and form filling
Permit form filling
Time Stamping Settings...
Encryption Settings...

Certified signature



Certified by Test Certificate <test@test.com>, Organization, certificate issued by Secure Soft Private CA.

Signature Properties

Document certification is valid, signed by Test Certificate <test@test.com>.

Signed by: Test Certificate <test@test.com>

Reason: Not available

Signing Time: 2011/06/21 15:23:59 +03'00'

Location: Not available

Validity Summary

The Document has not been modified since it was certified.

Include the CRL Revocation Information on the PDF Signature

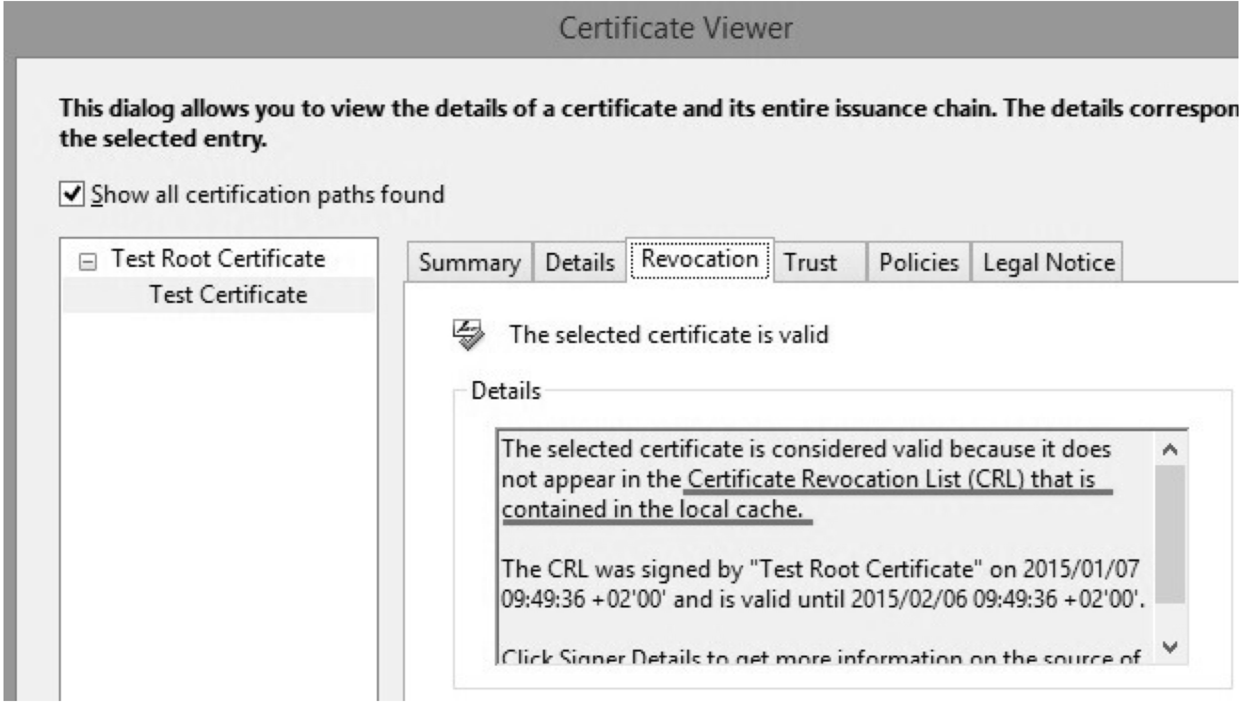
If the revocation information will not be available online, the digital signature cannot be verified by the Adobe Reader engine so it is recommended to include the CRL on the signature block.

This setting is available on the Digital Certificates window.

Note that some revocation information files (CRL) are very large so resulting signed file will proportionally larger.

PDF Stamper will try to include CRL for every digital certificate from the chain.

A PDF digital signature without revocation information



This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspon the selected entry.

☑ Show all certification paths found

The selected certificate is valid

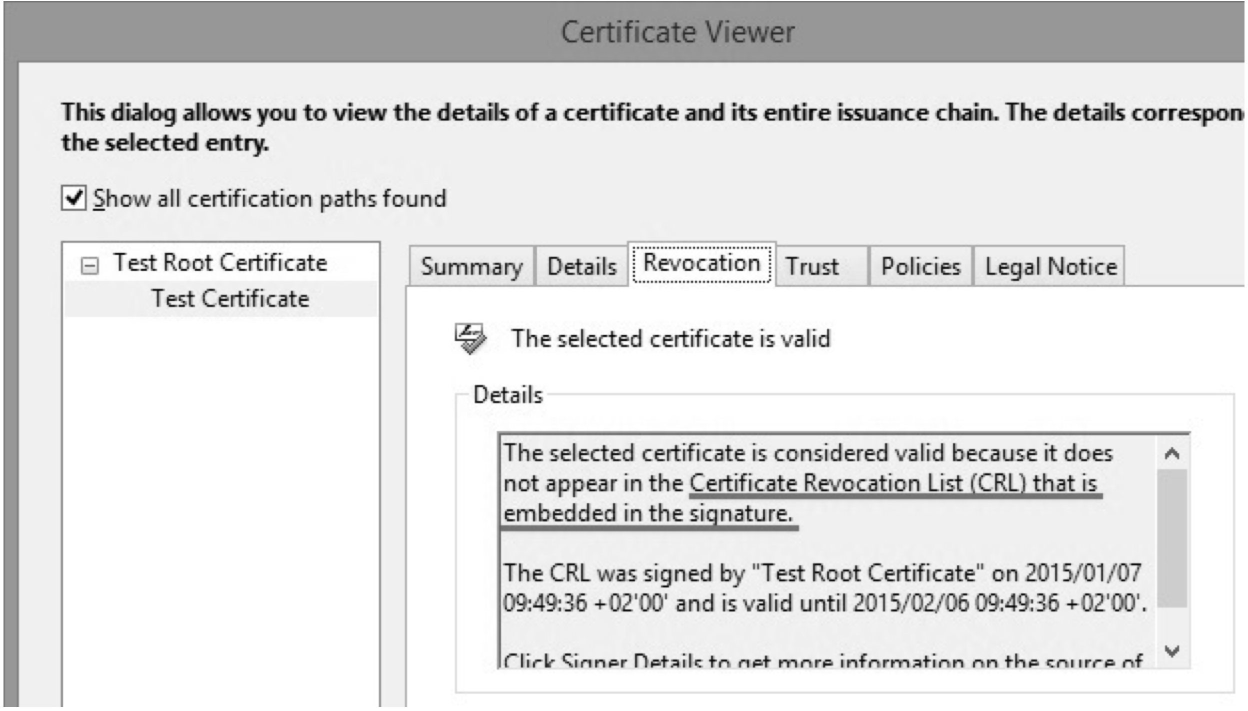
Details

The selected certificate is considered valid because it does not appear in the Certificate Revocation List (CRL) that is contained in the local cache.

The CRL was signed by "Test Root Certificate" on 2015/01/07 09:49:36 +02'00' and is valid until 2015/02/06 09:49:36 +02'00'.

Click Signer Details to get more information on the source of

A PDF digital signature that embeds the revocation information



This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspon the selected entry.

☑ Show all certification paths found

The selected certificate is valid

Details

The selected certificate is considered valid because it does not appear in the Certificate Revocation List (CRL) that is embedded in the signature.

The CRL was signed by "Test Root Certificate" on 2015/01/07 09:49:36 +02'00' and is valid until 2015/02/06 09:49:36 +02'00'.

Click Signer Details to get more information on the source of

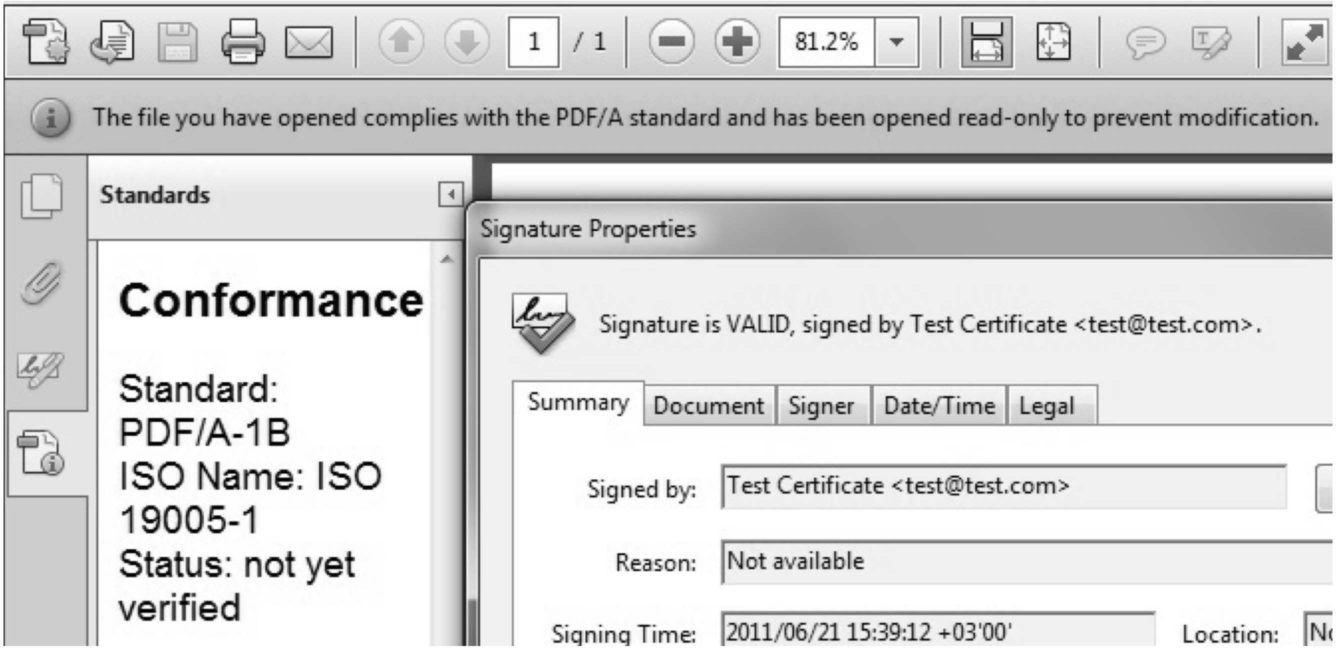
PDF/A Standard

PDF/A is a file format for the long-term archiving of electronic documents. It is based on the PDF Reference Version 1.4 from Adobe Systems Inc. (implemented in Adobe Acrobat 5 and latest versions) and is defined by ISO 19005-1:2005.

PDF Stamper can digitally sign PDF/A files.

Observation: In order to save a PDF/A file, all fonts used on the PDF document must be embedded (including the font used on the digital signature rectangle). The digital signature font can be set on the Signature Appearance section.

PDF/A-1b document with digital signature



The file you have opened complies with the PDF/A standard and has been opened read-only to prevent modification.

Standards

Conformance

Standard: PDF/A-1B
ISO Name: ISO 19005-1
Status: not yet verified

Signature Properties

Signature is VALID, signed by Test Certificate <test@test.com>.

Signed by: Test Certificate <test@test.com>

Reason: Not available

Signing Time: 2011/06/21 15:39:12 +03'00'

Location: N

Time Stamping

Time Stamp the PDF Digital Signature

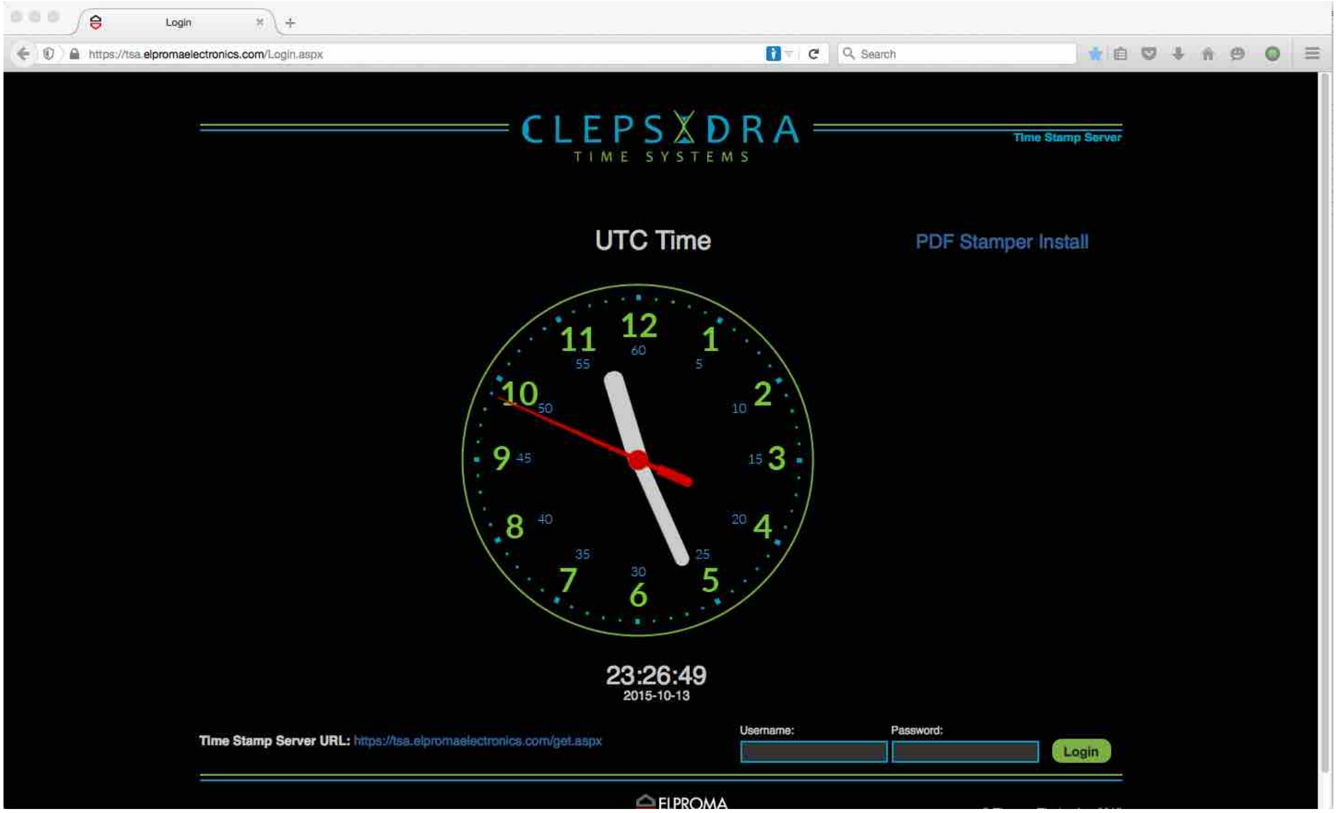
Timestamping is an important mechanism for the long-term preservation of digital signatures, time sealing of data objects to prove when they were received, protecting copyright and intellectual property and for the provision of notarization services.

To add time stamping information to the PDF digital signature you will need access to a RFC 3161 time stamping server (TSA).

A fully functional 100% FREE version of our TSA Authority is available for testing purposes at this link:

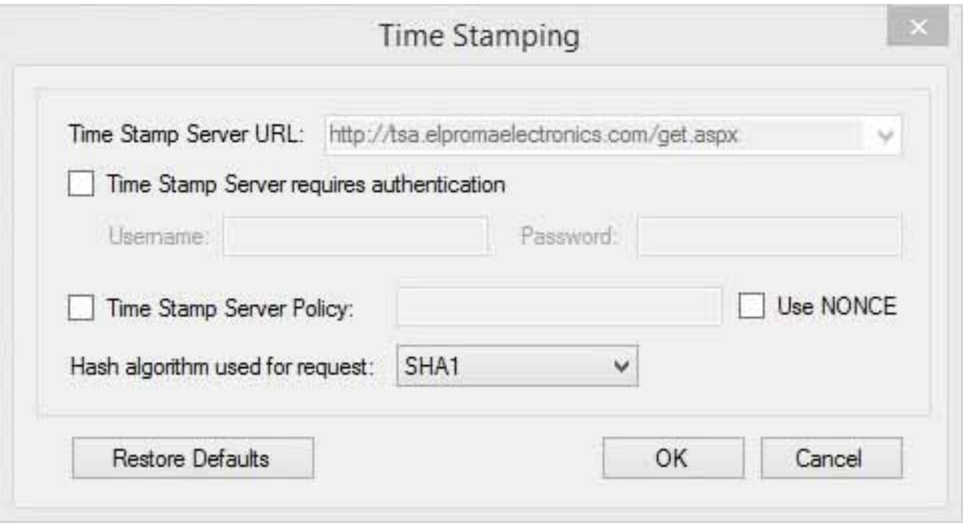
https://tsa.elpromaelectronics.com/get.aspx

(no credentials are needed).



Time Stamp Server URL: https://tsa.elpromaelectronics.com/get.aspx

The Time Stamping options can be configured on the *Time Stamping* section.



Time Stamp Server URL: http://tsa.elpromaelectronics.com/get.aspx

□ Time Stamp Server requires authentication

Username: Password:

□ Time Stamp Server Policy: □ Use NONCE

Hash algorithm used for request: SHA1

Nonce and Policy

The **Nonce**, if included, allows the client to verify the timeliness of the response when no local clock is available. The nonce is a large random number with a high probability that the client generates it only once (e.g., a 64 bit integer).

Some TSA servers require to set a **Time Stamp Server Policy** on the Time Stamp Requests. By default, no Time Stamp Server Policy is included on the TSA request.

Validating the Time Stamp Response on Adobe

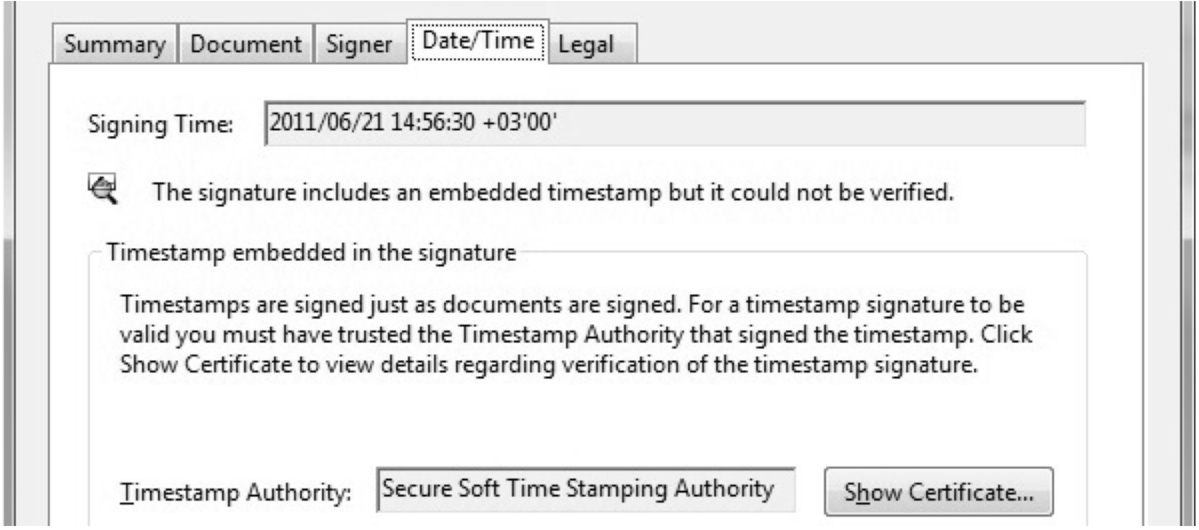
As digital signatures certificates, the time stamping responses are signed by a certificate issued by a Certification Authority.

If the time stamping certificate (or the Root CA that issued the time stamping certificate) is not included in Adobe Store, the time stamping response could not be verified when a user open a document with Adobe Reader (see example).

This behavior has nothing to do with the signing engine but with the Adobe certification validation procedure.

To validate the signing certificate in Adobe use the methods described on this document: http://www.clepsydratime.com/file_upl/PDF/ValidatingDigitalSignaturesInAdobe.pdf

Not verified timestamp



Signing Time: 2011/06/21 14:56:30 +03'00'

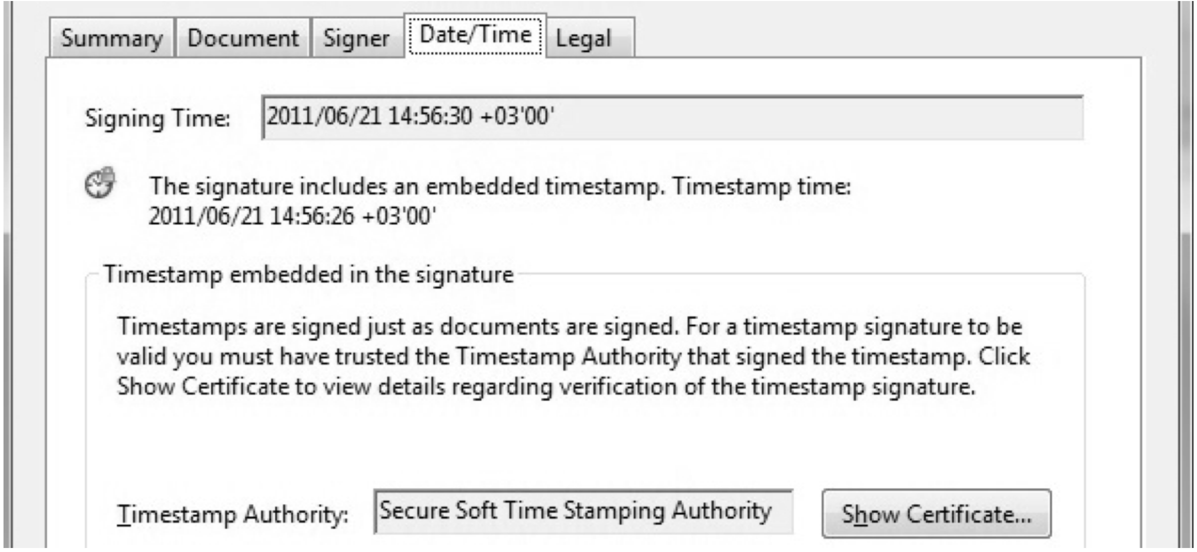
The signature includes an embedded timestamp but it could not be verified.

Timestamp embedded in the signature

Timestamps are signed just as documents are signed. For a timestamp signature to be valid you must have trusted the Timestamp Authority that signed the timestamp. Click Show Certificate to view details regarding verification of the timestamp signature.

Timestamp Authority: Secure Soft Time Stamping Authority

Trusted time stamping response



Signing Time: 2011/06/21 14:56:30 +03'00'

The signature includes an embedded timestamp. Timestamp time: 2011/06/21 14:56:26 +03'00'

Timestamp embedded in the signature

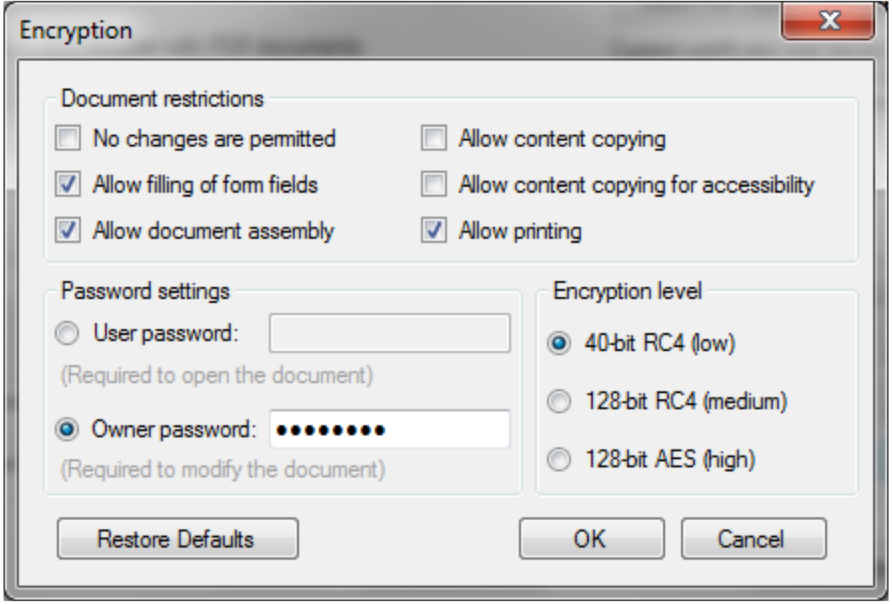
Timestamps are signed just as documents are signed. For a timestamp signature to be valid you must have trusted the Timestamp Authority that signed the timestamp. Click Show Certificate to view details regarding verification of the timestamp signature.

Timestamp Authority: Secure Soft Time Stamping Authority

Encryption

If you want to protect the signed document by preventing actions like printing or content copying you must encrypt it. The document can be encrypted using passwords from *Encryption* section.

Encryption settings



Encryption

Document restrictions

☐ No changes are permitted

☑ Allow filling of form fields

☑ Allow document assembly

☐ Allow content copying

☐ Allow content copying for accessibility

☑ Allow printing

Password settings

○ User password:

(Required to open the document)

● Owner password: ●●●●●●●●●

(Required to modify the document)

Encryption level

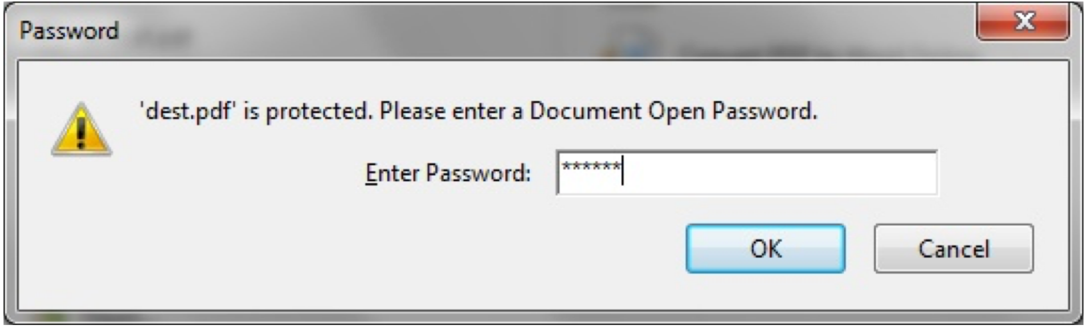
● 40-bit RC4 (low)

○ 128-bit RC4 (medium)

○ 128-bit AES (high)

If the PDF document is signed and encrypted with an *User Password,* when the document is opened in PDF reader, the PDF document password must be entered.

Password is required to open the document



Password

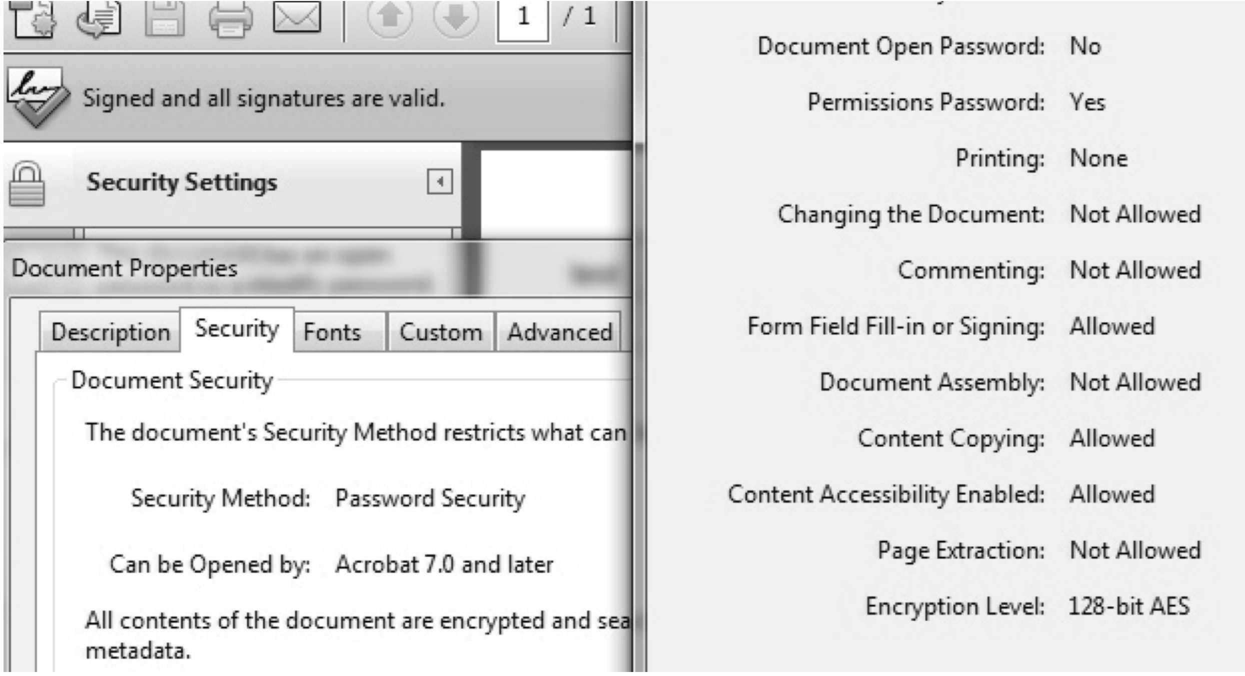
'dest.pdf' is protected. Please enter a Document Open Password.

Enter Password: ******

Owner Password is used to set the password that protects the PDF document for printing or content copying.

When the signed and encrypted document is opened in a PDF reader, the security settings are shown like below.

Security settings for a digitally sign and encrypted document



Signed and all signatures are valid.

Security Settings

Document Properties

Document Security

The document's Security Method restricts what can

Security Method: Password Security

Can be Opened by: Acrobat 7.0 and later

All contents of the document are encrypted and sea
metadata.

Document Open Password: No

Permissions Password: Yes

Printing: None

Changing the Document: Not Allowed

Commenting: Not Allowed

Form Field Fill-in or Signing: Allowed

Document Assembly: Not Allowed

Content Copying: Allowed

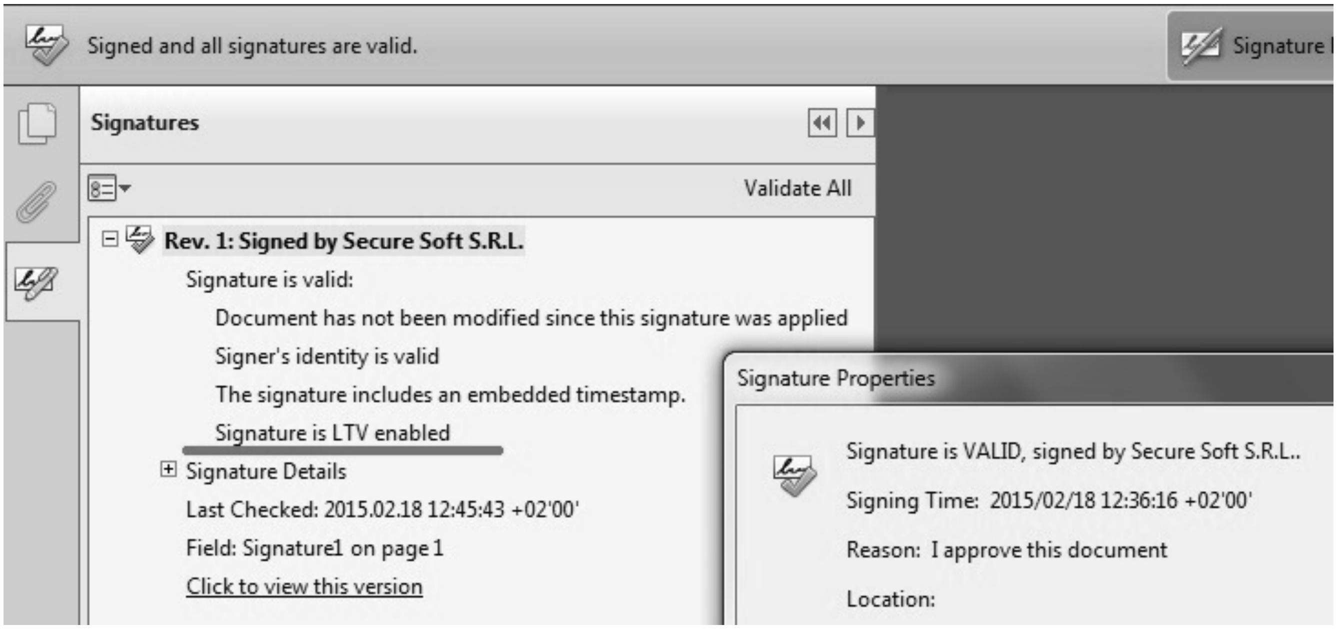
Content Accessibility Enabled: Allowed

Page Extraction: Not Allowed

Encryption Level: 128-bit AES

LTV Signatures (Long Term Validation)

PAdES recognizes that digitally-signed documents may be used or archived for many years – even many decades. At any time in the future, in spite of technological and other advances, it must be possible to validate the document to confirm that the signature was valid at the time it was signed – a concept known as Long-Term Validation (LTV).



Signed and all signatures are valid.

Signatures

Rev. 1: Signed by Secure Soft S.R.L.

Signature is valid:

Document has not been modified since this signature was applied

Signer's identity is valid

The signature includes an embedded timestamp.

Signature is LTV enabled

Signature Details

Last Checked: 2015.02.18 12:45:43 +02'00'

Field: Signature1 on page 1

Click to view this version

Signature Properties

Signature is VALID, signed by Secure Soft S.R.L..

Signing Time: 2015/02/18 12:36:16 +02'00'

Reason: I approve this document

Location:

In order to have a LTV signature, be sure that on the Digital Certificates settings, the checkbox *Include certificate revocation information – Long Term signature (LTV)* is checked.

Batch Signatures (Automatically Made Without User Intervention)

By default, PDF Stamper is installed on this location:

C:\Program Files\PDF Stamper\PDF Stamper.exe.

The command line parameters are:

```
PDF Stamper.exe <source file | folder> <destination file | folder> [<XML configuration file>]
```

To automatically sign a **PDF file**, use the following command:

```
c:\Program Files\PDF Stamper>"PDF Stamper.exe" c:\InputFile.pdf c:\SignedFile.pdf
```

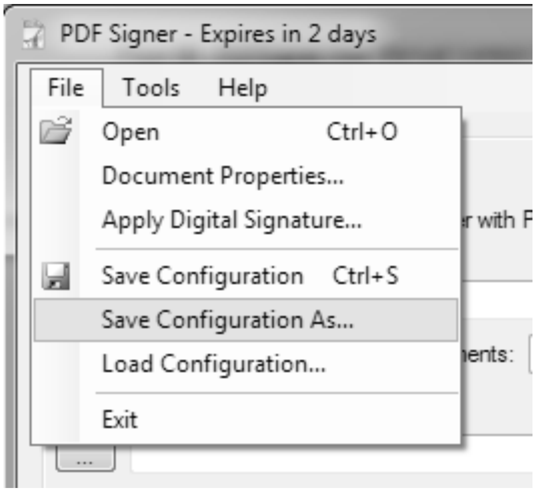
To automatically sign a **folder** that contains PDF files, use the following command:

```
c:\Program Files\PDF Stamper>"PDF Stamper.exe" c:\InputFolder c:\OutputFolder
```

Custom Configuration

In some cases, you will need a different signature configuration (e.g. different signature appearance and digital certificates) for different PDF files/folders.

To save a specific configuration, go to *File – Save Configuration As* and save the configuration on a file. Later, you can use that file in batch mode to apply different signature configuration on your signed PDF file.



To automatically sign a **folder** that contains PDF files, using a custom configuration, use the following command:

```
"PDF Stamper.exe" c:\InputFolder c:\OutputFolder c:\config-client2.xml
```